DOD 5200.2-R, JUNE 2002 (DRAFT) - AP6. APPENDIX 6

DoD 5200.2-R, June 2002 (draft)
AP6. APPENDIX 6

POSITIONS REQUIRING ACCESS TO DoD INFORMATION TECHNOLOGY (IT) SYSTEMS AND NETWORKS

AP6.1. PURPOSE

This appendix establishes standard categories for positions within the Department of Defense and within defense contractor facilities that could be exploited by the individuals who are assigned to positions that directly or indirectly affect the operation of unclassified information technology (IT) resources and systems that process For Official Use Only (FOUO) and other controlled unclassified information. Such positions are referred to as IT and IT-related positions. These categories are to be used to distinguish and categorize the impact that individuals with certain IT privileges could have on DoD functions and operations.

The appendix also includes investigative and adjudicative requirements associated with these positions. The requirements of this appendix, are to be applied to all IT positions, whether occupied by DoD civilian employees, military personnel, consultants, contractor personnel or others affiliated with DoD (e.g., volunteers).

In today's environment, personnel in nearly every work situation use a computer to perform their assigned duties. In most of these situations, IT systems and resources are used as tools that enhance the incumbent's ability to accomplish their assignments. While these positions may require knowledge of various applications and skill in using available IT resources, the incumbents are not involved in developing, delivering, or supporting IT systems and services, or safeguarding sensitive data within such systems. Such IT users do not normally occupy IT positions and are not subject to the requirements of this Appendix. Their access, however, will be subject to established disclosure and security policies, such as described in section AP6.6.

AP6.2. DEFINITIONS

Information Technology (IT) Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Limited Privileged Access Privileged access with limited scope, e.g., an authority to change user access to data or system resources for a single information system (IS) or physically isolated network.

Non-Privileged Access User level access, i.e., normal access given to a typical user. Generally, all access to system resources is controlled in a way that does not permit those controls/rules to be changed or bypassed.

Controlled Unclassified Information Unclassified information that requires application of controls and protective measures for a variety of reasons. Examples of controlled unclassified information include, but are not limited to, the following categories:

(1) For Office Use Only (FOUO): Information that may be withheld from mandatory public disclosure under the Freedom of Information Act (FOIA) (reference (ii)).

(2) Unclassified Technical Data: Data related to critical technology with military or space application which may not be exported lawfully without approval, licenses or authorization under the Arms Export Control Act.

(3) Department of State Sensitive But Unclassified (SBU): Information which originated from the Department of State (DoS) which has been determined to be SBU under appropriate DoS information security polices.

(4) Foreign Government Information: Information provided by a foreign government or governments, an international organization of governments or any element thereof, with the expectation that the information or source of the information, or both, are to be held in confidence.

(5) Privacy Data: Personal and private information (e.g., individual medical information, home address and telephone number, social security number) as defined in the Privacy Act (reference (pp)).

(6) Sensitive Information (Computer Security Act of 1987): Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act) (reference (pp)), but which has not been specifically authorized under criteria established by executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information in routine DoD payroll, finance, logistics, and personnel management systems.

Privileged Access Authorized access that provides capability to alter the properties, behavior or control of the information system/network. It includes, but is not limited to, any of the following types of access:

(1) “Super user,” “root,” or equivalent access, such as access to the control functions of the information system/network, administration of user accounts, etc.

(2) Access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multiplexers, and other key information system/network equipment or software.

(3) Ability and authority to control and change program files, and other users’ access to data.

(4) Direct access to operating system level functions (also called unmediated access) which would permit system controls to be bypassed or changed.

(5) Access and authority for installing, configuring, monitoring or troubleshooting the security monitoring functions of information systems/networks (e.g., network/system analyzers; intrusion detection software; firewalls) or in performance of cyber/network defense operations.

AP6.3. GENERAL GUIDANCE

AP6.3.1. Defense in-depth requires, and DoD Directive 5200.28 (reference (tt)) specifies, that information systems/networks be safeguarded through use of a mixture of administrative, procedural, physical, communications, emanations, computer, and personnel security measures, that together achieve the requisite level of security. As DoD becomes increasingly dependent upon information technology to execute the DoD mission, ensuring the trustworthiness of all personnel, including temporary, seasonal, and intermittent employees, contractors, and volunteers, who have access to IT systems and networks is critical.

AP6.3.2. The type of access authorized (privileged, limited privilege, or non-privileged) is key to determining the level of trustworthiness required. It measures an incumbent’s capability to effect the operation of DoD information systems and networks and potential to adversely impact the Department’s overall security posture or ability to execute its mission.

AP6.3.3. The requirements of this appendix are intended to enhance the security of DoD IT systems and networks and to safeguard controlled unclassified information. In those cases where controlled unclassified information (e.g., critical technologies and Privacy Act data) is maintained in contractor owned and operated IT systems that have no interconnection (including data feeds) with DoD IT systems or networks, other safeguards (e.g., non-disclosure agreements, training) authorized in accordance with other applicable guidance may be used at the IT-III level in lieu of background investigations to mitigate the risks associated with the loss/misuse or unauthorized access to or modification of controlled unclassified information.

AP6.3.4. Level of access granted must be supported by the appropriate investigative basis/authority for holding a position at that level.

AP6.3.5. This policy applies to contractors and consultants who require access to DoD systems and networks and shall be implemented through incorporation in their contracts.

AP6.3.6. For cases in which the investigative requirements for IT access exceed the investigative requirements for access to classified information/security clearance requirements, the higher requirement must be met.

AP6.3.7. Users of this appendix are also cautioned that other policies may levy additional requirements that must be met prior to assignment to a particular position requiring IT access. For example, each Designated Approving Authority (DAA), Information System Security Managers (ISSM), and Information System Security Officer (ISSO) must be a U.S. citizen; DAAs additionally must be U.S. Government personnel. Similarly, Verifying Officials (VO) and personnel appointed to operate Certificate Management Authority (CMA) equipment in support of DoD Public Key Infrastructure (PKI) must be U.S. citizens. It is the user's responsibility to be aware of additional requirements pertinent to the specific IT environment and to factor those requirements into this process at the appropriate places.

AP6.3.8. A phased implementation plan beginning in FY03 will be issued via memorandum in order to provide DoD Components sufficient time to comply with the policy contained in this Appendix.

AP6.4. IT ACCESS CATEGORIES

This paragraph defines IT access categories based on level of information system/network access required to execute responsibilities of the position and the associated potential for adverse impact on the DoD mission. DoD components are responsible for designation of each position as requiring privileged, limited privilege, or non-privileged access. Positions may be categorized at the higher level as needed to account for ability to impact overall network/system security posture, intended system behavior, or appropriate content. DoD agencies that issue contracts requiring access to DoD IT systems/network shall provide specific guidance to their contractors regarding the categorization of contractor positions and the investigative requirements of this Regulation.

AP6.4.1. IT-I Position. Incumbent of this position has privileged access to networks and information systems, system security and network defense systems, or to system resources. Duties are broad in scope and authority and provide access to the U.S. Government, DoD, or Component mission critical systems. The potential exists for exceptionally serious adverse impact on U.S. Government, DoD, Component or private sector information and/or operations, with worldwide or government-wide effects. Incumbent may also be responsible for unsupervised funds disbursements or transfers or financial transactions totaling over $10M per year.

AP6.4.2. IT-II Position. Incumbent of this position has limited privileged access, but duties are of considerable importance to the DoD or DoD Component mission, and the incumbent is under the supervision of an individual in a higher trust position (IT-I). For example, individuals in these positions may have ability to impact a limited set of explicitly defined privileged functions, such as privileged access confined to large portions of an IT or to a local network physically isolated from other DoD or publicly accessible networks. The potential exists for moderate to serious adverse impact on DoD or Component information or operations. Incumbent may also be responsible for monitored/audited funds disbursements or transfers or financial transactions totaling less than $10M per year.

AP6.4.3. IT-III Position. Incumbent in this position has non-privileged access to one or more DoD information systems/applications. IT-III incumbents can receive, enter and/or modify information in an information system/application or database to which they are authorized access. Users have access only to that data/information and those applications/ networks to which the incumbent is explicitly authorized or has need-to-know and cannot alter those or other users' authorizations. Positive security measures and configuration management ensures that the incumbent can assume only explicitly authorized roles and privileges. The potential exists for limited adverse impact on DoD, Component or unit information or operations. Incumbent may also be responsible for financial operations subject to routine supervision or approval, but has no funds disbursement or transfer capabilities.

AP6.5. TYPICAL CATEGORY ASSIGNMENT BY IT SPECIALTY

AP6.5.1. DoD components are responsible for categorization of each IT position at the highest level required by the specific duties, risks, and safeguards in place after analysis of the position's aggregated privileges, scope and levels of independence. Positions may be categorized at higher or lower levels as needed to account for ability to impact overall network/system security posture, intended system behavior, or appropriate content. However, when level of privilege and other position characteristics appear to indicate differing levels of categorization, the higher categorization assignment should be used.

AP6.5.2. The following are typical category assignments for each IT specialty title defined in the OPM Position Classification Standard "Administrative Work in the Information Technology Group, GS-2200" (http://www.opm.gov/FEDCLASS/gs2200a.pdf). Other IT-related positions should be categorized based on the particular set of duties and responsibilities of the position and the scope, and level of privileges authorized.

a. Policy and Planning (PLCYPLN) – IT-III (IT-II if responsible for information security/ information assurance program or if individual also has privileged access)

b. Security (INFOSEC) – IT-I (IT-II if primarily policy, planning or awareness focused)

c. Systems Analysis (SYSANALYSIS) – IT-III (IT-II if responsible for information security/information assurance systems)

d. Applications Software (APPSW) – IT-I, -II, or –III depending on specifics of application (IT-I if responsible for information security/information assurance applications)

e. Operating Systems (OS) – IT-II (IT-I if incumbent acts independently, without oversight/review)

f. Network Services (NETWORK) – IT-I or IT-II (depending on the scope of network--as defined by criticality of or impact on Department or Federal government mission, geographic reach, and/or major or significant impact on other government agencies and/or the private sector--and level of privileges)

g. Data Management (DATAMGT) – IT-III (IT-II if responsible for safeguarding sensitive data/information)

h. Internet (INET) – IT-II (IT-I if privileged access to network functions)

i. Systems Administration (SYSADMIN) – IT-I (IT-II if stand-alone system or if ability to compromise limited to system/network operation)

j. Customer Support (CUSTSPT) – IT-III (IT-I if privileged access; or IT-II if ability to set/change user access privileges (scope and level sensitive))

Other activities or specialties that may have significant IT duties include the following:

a. Computer Clerk and Assistant (GS-335) or Computer Operation (GS-332) – typically IT-III, but may be higher if there is access to system/network control functions.

b. Telecommunications (GS-391) (e.g., computer network analysts; data communications) – use appropriate IT specialty in subparagraph AP6.5.2 above.

c. Computer engineer (GS-0854) – generally hardware focused; typically IT-III, but specific categorization depends on function and application of the specific hardware/component (e.g., chip/board design may be IT-I), degree of supervision/review by higher authority, etc.

d. Computer Science (GS-1550) – categorization depends on specific duties/ responsibilities; use appropriate IT specialty in subparagraph AP6.5.2 above where possible.

e. Criminal Investigating (GS-1811) – Law enforcement activities associated with computer/network crime (e.g., forensic analysis; criminal investigation) – categorization depends upon required level of access (e.g., privileged/non-privileged).

f. Miscellaneous Management and Program Analysis (GS-343) and other scientists, subject matter experts, and professionals -- depends upon required level of access (e.g., privileged/nonprivileged).

g. Technical editors and other subject matter experts who develop web pages, but whose primary expertise is not technical knowledge of Internet systems, services, and technologies – categorize under "Internet" IT specialty; if non-privileged access, may be assigned IT-III designation

h. Miscellaneous IT specialists (As required by specifics of new technology/ evolving specialty area) – use appropriate IT specialty in subparagraph AP6.5.2 above where possible.

i. Threat and vulnerability assessment (e.g., red-teams; penetration testing) - determined by the purpose and scope of the assessment objective and required level of access.

j. Certificate Management Authorities (CMA) to include Verifying Officials (VO) - typically IT-II, but may be higher if operating CMA equipment associated with Public Key Infrastructure operating above the DoD Class 4 assurance level.

AP6.6. ACCESS BY NON-U.S. CITIZENS

AP6.6.1. Access to unclassified information by a non-U.S. citizen shall only be permitted in accordance with applicable disclosure policies (e.g. DoD Directive 5230.9 (reference (uu)), DoD Directive 5230.25 (reference (vv)), DoD 5400.7-R (reference (ii)) and U.S. statutes (e.g., Arms Export Control Act). A non-U.S. citizen shall not be assigned to a DoD IT position requiring access to information that is not authorized for disclosure by the U.S. organization that originated the information to his or her country of citizenship.

AP6.6.2. Non-U.S. citizens assigned into DoD IT positions are subject to the investigative requirements outlined in section AP6.7. For non-U.S. citizens employed outside of the United States in countries hosting U.S. forces, investigative requirements are outlined in subparagraph C3.5.4.

AP6.6.2.1. A non-U.S. citizen may be assigned to an IT-I position if the head of the DoD Component or Agency that owns the system/information/network approves the assignment in writing. The written approval must be on file before requesting the required investigation. The required investigation must be completed and favorably adjudicated prior to authorizing IT-I access to DoD systems/networks. Interim access is not authorized. Every effort shall be made to minimize, and where possible eliminate, the number of non-U.S. citizens employed in IT-I positions. However, compelling reasons may exist to grant such access in those circumstances where a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed for a specific DoD requirement and for which a suitable U.S. citizen is not available.

AP6.6.2.2. Non-U.S. citizens may hold/be authorized access to IT-II and IT-III. The required investigation must be completed and favorably adjudicated prior to authorizing IT-II and IT-III access to DoD systems/networks. Interim access is not authorized.

AP6.6.3. By December 1 following the end of each fiscal year, the DoD Components will provide a report to the DASD(S&IO), OASD(C3I), containing the following data:

AP6.6.3.1. Number of non-U.S. citizens occupying a IT-I position, broken out by location, i.e., CONUS or OCONUS;

AP6.6.3.2. For each location (CONUS or OCONUS), the number of individuals by nationality.

AP6.7. LEVEL OF BACKGROUND INVESTIGATION

The required investigations for all IT-I, IT-II and IT-III positions are outlined below.

POSITION CATEGORY	CIVILIAN	MILITARY	CONTRACTOR	NON-U.S. CITIZEN*
IT-1	SSBI	SSBI	SSBI	SSBI, if approval granted
IT-II	NACI	NACLC	NACLC	NACLC
IT-III	NACI	NAC	NAC	NAC

*Investigative requirements for non-U.S. citizens outside the U.S. are outlined in subparagraph C3.5.4.

Assignment (including assignments due to accretion of duties) of current DoD employees, military personnel, consultants and contractors to positions with increased access privileges requires verification of the appropriate investigative basis/authority for holding a position of that level of sensitivity.

AP6.8. REQUESTS FOR INVESTIGATION

AP6.8.1. IT investigations are to be submitted to OPM using the SF86. The form is to be completed only after a conditional offer of employment.

AP6.8.2. Each requester will need to establish a submitting office number (SON) with OPM before requesting an investigation. Appendix 2 contains guidance on submitting investigations to OPM. Your office must place this SON code on each request submitted to OPM.

AP6.8.3. Completed investigations are to be returned to OPM for a trustworthiness determination. To ensure the completed investigation is properly returned to OPM, the designation - OM25 - must be reflected in Item L when completing the Agency Use Block section.

AP6.8.4. When completing Item N, contractor requesters must indicate the appropriate billing code of the DoD contracting activity.

AP6.8.5. For cases in which the investigative requirements for IT access exceed the investigative requirements for access to classified information; the higher requirement must be met.

AP6.9. INTERIM ASSIGNMENT

AP6.9.1. Individuals, except non-U.S. citizens, to include temporary, intermittent and seasonal personnel, may be assigned to IT-I, IT-II, or IT-III positions on an interim basis prior to a favorable adjudication of the required personnel security investigation only after the conditions specified below have been met. Interim access is not authorized for non-U.S. citizens.

AP6.9.1.1. IT-I:

AP6.9.1.1.1. Favorable completion of the NAC (current within 180 days)

AP6.9.1.1.2. Initiation of an SSBI/favorable review of SF86

AP6.9.1.2 IT-II:

AP6.9.1.2.1. A favorable review of local personnel, base/military, medical, and other security records as appropriate

AP6.9.1.2.2. Initiation of a NACI (for civilians) or NACLC (for military and contractors), as appropriate/favorable review of SF86

AP6.9.1.3. IT-III:

AP6.9.1.3.1. A favorable review of local personnel, base/military, medical, and other security records as appropriate

AP6.9.1.3.2. Initiation of a NACI (for civilians) or NAC (for military and contractors), as appropriate/favorable review of SF86

AP6.9.2. For DoD civilian and military personnel, the approval for interim assignment shall be made by the security manager at the requesting activity. For DoD contractor personnel, approval authority for interim assignment reside with the government sponsor's security manager/official, but may be delegated to the contractor's senior security official with the approval of the Head of the DoD Component or Agency that owns the system/information.

AP6.10. ADJUDICATION

AP6.10.1. Completed investigations will be forwarded to OPM (SOI: OM25) for a trustworthiness determination. Adverse cases will be sent to DOHA for final action. The submitting entity will be notified in writing regarding the results of the OPM/DOHA decision. The guidelines in Appendix 5 and procedures in Chapter 9 will serve as the basis for most decisions. In certain cases, status as a non-U.S. citizen is not an automatic disqualified. For contractor personnel, trustworthiness determinations are outside the provisions of the NISP.

AP6.10.2. All trustworthiness determinations will be entered into JPAS.

AP6.11. REINVESTIGATION

Individuals occupying a position requiring IT access shall be subject to an aperiodic reinvestigation under the forthcoming ACES (estimate June 2003).

AP6.12. PRIOR BACKGROUND INVESTIGATIONS

If an individual previously has been subject to background investigative and adjudicative requirements, depending on the age of the investigation those requirements may not need to be duplicated for IT access. Investigative criteria for DoD personnel and contractors/ consultants who have had prior background investigations are outlined in the table below.

IT Position Category/Investigative Equivalency Table
DoD Civilian and Military Personnel, Contractors, and Consultants

If Position Category is:	***Individual has/had the following investigation:***	***And the age of the investigation is:***	***Then the investigation required is:***
IT-I	SSBI SSBI-PR	< 5 yrs	None
		> 5 yrs	SSBI-PR
	SBI BI LBI MBI NACLC ANACI NAC NACIC ENTNAC	Regardless of age of the investigation	SSBI
IT-II	SSBI SSBI-PR SBI BI LBI MBI NACLC ANACI NACIC	< 10 yrs	None
		> 10 yrs	NACLC
	ENTNAC NAC	Regardless of age of the investigation	NACLC (contractor, military) NACI (civilian)
IT-III	SSBI SBI BI SSBI-PR LBI MBI ANACI NACLC NAC NACIC ENTNAC	< 15 yrs	None
		> 15 yrs	NAC (contractor, military) NACI (civilian)

AP6.13. TRAINING AND AWARENESS REQUIREMENTS

DoD Components must ensure that individuals with access to DoD IT systems and networks receive the requisite information assurance, security awareness, and functional competency training as required by their designated level of access and scope of duties, and that the training is documented in individual personnel files. Understanding the threats, system vulnerabilities, and protective measures required to counter such threats are key features to a core information assurance awareness program at each IT access level.